The Department of Energy Enterprise Risk Management Model

Using the Risk Assessment Tool to Prepare a Justification Memorandum for the Development and Revision of Departmental Directives

Enterprise Risk Management (ERM) Model - Background

- On January 14, 2011, Secretary Chu issued a memorandum outlining goals for improving mission execution.
- An Integrated Management System (IMS) Team consisting of both Federal managers, subject matters experts and contractors has been engaging leadership across the Department to develop a plan for creating and implementing an Enterprise Risk Management (ERM) Model.
- The benefit of ERM is that it will better equip the Department to manage performance and make risk-informed decisions.

Enterprise Risk Management (ERM) Model - Principles

- The Department will defer to external standards or regulations whenever possible to enable our contractors to remain competitive and equipped to best manage our laboratories.

- DOE will only develop Department-specific requirements when external standards or regulations cannot adequately manage risk and performance within DOE.

- All DOE developed requirements documents, or directives, that cut across the Departmental Elements lines of authority must utilize the ERM Model which will ensure the Department makes decisions that are risk-informed rather than risk-adverse.

Five Steps of the ERM Review Process

1. **Risk Identification.** What can go wrong? List all possible events that could occur in a subsystem if there are no controls. Once risks are identified, combine like risks according to the following key areas impacted by the risks: people, mission, physical assets, financial assets, and customer/stakeholder trust.
2. **Risk Analysis.** What is the likelihood and impact? Rate risks according to probability and impact.
3. **Requirements Identification.** What is in place to prevent it? List all controls that would exist without DOE subsystem-specific controls.
4. **Controls Identification.** What else is needed to control the risk? Where there is a significant or extreme risk rating, list gaps between existing risks and existing controls.
5. **Risk Registry.** What documentation is needed so that the logic and conclusions are clear? Create a register that documents the results of the risk evaluation, including the events, probabilities, impacts, and risk management strategy.

Risk Identification and Analysis

For each subsystem a group of senior level staff and subject matter experts complete the following-

1. **Risk Identification.** What can go wrong? What events can have an impact on people, mission, physical assets, financial assets, and customer/stakeholder trust? A risk can also be a missed opportunity for improving effectiveness and efficiency.
2. **Risk Analysis.** Look at the subsystem in the context of existing external controls. If there were no DOE-specific controls what is the probability and impact of specific risks?

		Impact			
		Negligible	Low	Medium	High
Probability	Certain	Minor	Moderate	Extreme	Extreme
	Likely	Minor	Moderate	Significant	Extreme
	Possible	Minor	Moderate	Significant	Extreme
	Unlikely	Minor	Minor	Moderate	Significant
	Rare	Minor	Minor	Minor	Moderate

Requirements Identification

3. **Requirements Identification.** What is in place to prevent it? List all controls that would exist without DOE subsystem-specific controls.
4. **Controls Identification.**

   What else is needed to control the risk? Where there is a significant or extreme risk rating, list gaps between existing risks and existing external controls. Defer to existing external controls and standards whenever possible.

Cost Effective Risk Management

- What is the most effective method for bringing risk down to an acceptable level?
- Are the controls most expensive than the risk?

Minor – risk acceptance may be preferred

Moderate – existing controls may be adequate

Significant – may need to add more controls

Extreme – more controls likely needed

Risk Register

5. Risk Registry

- Clearly document the analysis of identified risks, existing controls, and proposed controls to address any serious gap between existing controls and risk.
- Risk Mitigation Options – Acceptance, Monitoring, Mitigation, and Avoidance
- Evaluate the costs of various mitigation techniques compare the cost/benefit of the risk

Risk/ Opportunity	Risk Level	Potential Cost/Benefit	External Control(s)	Proposed Mitigation Technique	Internal Control (if needed)
Identify specific risks and their risk level	Minor, Moderate, Significant and Extreme – based on the probability and impact chart.	Give a rough estimate of the magnitude of the cost/benefit of the risk/opportunity without DOE-specific controls.	List all external controls that help address the risks and opportunity identified.	Based on any gap between the risk/opportunity and existing controls, what strategy should DOE adopt?	List all internal controls needed to effectively and efficiently address gaps between risks and external controls.

Sample Risk Analysis

Risk Assessment for DOE O 333.1, *Workforce Discipline*					
Risk/ Opportunity	**Risk Level**	**Potential Cost/Benefit**	**External Control(s)**	**Proposed Mitigation Technique**	**Internal Control**
1. Loss of employee trust and low morale from perception of favoritism. (Failure to take the appropriate disciplinary action; arbitrary and inconsistent discipline; failure to address misconduct at the earliest possible stage.)	Extreme	Significant time commitment for managers and costs to the department in excess of $1M	5 U.S.C., 5 CFR, Part 752, MSPB, EEOC, DOE Inspector General (IG)	Mitigation	**A.** Disciplinary action must be taken for: (1) the purpose of correcting unacceptable conduct at work; (2) behavior that adversely affects job performance; (3) violations of laws, rules, or regulations; or (4) off-duty misconduct when there is a nexus between the misconduct and employment with DOE.
2. Disruption in the workplace	Significant	Moderate time commitment for all staff	5 U.S.C., 5 CFR, Part 752, MSPB, EEOC, DOE Inspector General (IG)	Monitoring	**B.** Contact Servicing HR offices before initiating disciplinary/adverse actions.
3. Embarrassment to the agency; potential political concerns.	Minor	Moderate time commitment for PR staff		Acceptance	

Please note: The sample above has been tweaked for instructional purposes.

Why is ERM important?

- **Integrated Strategy** - ERM is important because it supports the Department's strategy and our Management Principles including, "we will manage risk in fulfilling our mission".
- **Consistency-** Systematic approach for management and operations – how we make decisions, govern how we establish and implement requirements, and how we hold ourselves accountable .
- **Better Communication** - ERM will provide that framework for clearly articulate the processes we use for program execution, and governance.
- **Clear and Concrete Measures of Performance** - It will improve efficiency and allow DOE to consistently speak with one voice to our contractors, customers, and stakeholders.

Path Forward

1. Program Secretarial Officers can submit a request to the DRB to evaluate a subsystem
2. The DRB develops a Risk Assessment Team
3. Risk Assessment Team completes the ERM risk assessment tool
4. Writer develops/revises a directive incorporating any DOE-specific controls needed after the risk analysis
5. Regularly evaluate the effectiveness of the chosen risk mitigation techniques